Secure Mechanism for DYMO Routing Protocol by using Elliptic Curve Cryptography in Mobil Ad-hoc Networks

Rayala Upendar Rao
Department of Computer Science
Vignan University
Andhra Pradesh, India.

Daranasi Veeraiah
Department of Computer Science
Vignan University
Andhra Pradesh, India

ABSTRACT
Mobile ad hoc networks are wireless multi hop networks characterized by lack of centralization, in dynamic topologies. So there is a chance to get various types of attacks including denial of service attacks, which leads to consume the system resources like bandwidth, power and memory. To avoid these vulnerable attacks researchers proposed many schemes, but still those are possessing huge threats. Hence there is a necessity of new secure routing mechanism. So we introduced new secure mechanism by using Elliptic Curve Cryptography (ECC) with help of DYMO routing protocol. Here we implemented access control mechanism on ECC which ensure authentication and confidentiality. There by we can able to identify resource consumption attack and mitigates this by informing to other routing AGENT node about its identity and bootstrapping time. Here the main advantage with ECC is, it takes less memory provides great security and perfectly suitable for low power devices like mobile nodes. So the performance of the overall system is good compare with other secure routing mechanisms.

Keywords
Access Control, Resource consuming attacks, Security, Bootstrapping Time,DYMO, MANET.

1. INTRODUCTION
A "mobile ad hoc network" (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links --the union of which form an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

MANET nodes consist of sensing, data processing, and communication components and typically form ad hoc networks. Due to a lack of infrastructure support, each node acts as a router, forwarding data packets for other nodes. Mobile nodes periodically exchange the information about topology of the network. Every node has to take part in routing and replaying the message for other nodes. We can consider issuing ticket in local buses as a practical example for transferring packets in MANET. Ad hoc network applications are applied in battle fields, major disaster areas, conferences and the entertainment industry. Because of dynamic connectivity MANET has attracted a lot of attention recently. But it is vulnerable to attack due to its mobility and ad hoc nature. Generally, routing and network management has to be performed in MANET.

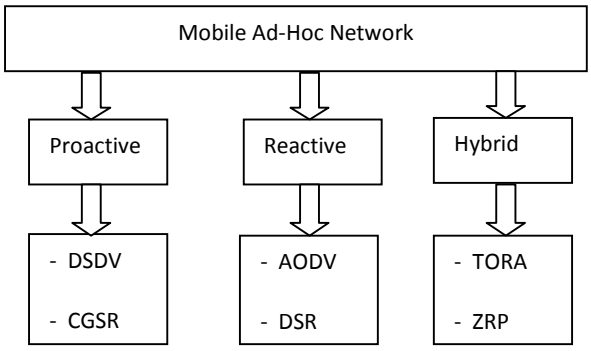

Figure1. MANET Protocol list

Many routing protocols have been developed and used at present. Based on the network topology and its strategy, routing protocols [3] have been classified into proactive, reactive and hybrid protocols. Proactive protocols are table driven which includes DSDV, CGSR, WRP, etc. It stores the information about the network in its routing table. Whenever it needs to communicate with other nodes, it uses the routing table and forwards the packets. It requires additional hardware or software requirements and routing table which has to be updated periodically to provide efficient service. But reactive protocols don't require it. Hence, it is termed as On-Demand routing protocol. It propagates to the nodes whenever it is necessary. So there is no need to maintain all information in routing table. It includes AODV, DSR, RSRP, etc. Hybrid protocols make use of both proactive and hybrid protocol. It includes TORA, ZRP, SSR, OORP, etc. Figure 1 show various protocols used in MANET.

Security is main concern in all communication networks. Ad hoc network should concentrate more on security due to its inherent nature. There is a possibility of many attacks like eavesdrop, forged packets and denial of service attacks. In the modern world, most of the user utilizes laptops, PDA and other mobile devices. There is a necessity of providing security to those mobile nodes for secure transmission of messages. Detection and prevention plays a major role in security in network. It is better to detect and prevent malicious node or packets without

affecting system Performance. This paper mainly focuses on how anomaly can be detected and prevented using DYMO protocol. To mitigate all these attacks we need complex asymmetric algorithms, but they will take huge amount of resources for implementing. Wireless MANET nodes are having limited, constrained capabilities and not suitable for complex asymmetric algorithms. Hence we consider ECC as better secure mechanism takes less bits and provides more security. There are many algorithms are implemented on ECC for various purposes. We consider two algorithms Elliptic Curve Digital Signature Generation Algorithm (ECDSA) and Elliptic Curve Diffie Hellman Algorithm (ECDHA). Here authentication can be achieve through ECDSA by providing digital signature for each node and establishment of key sharing between any pair of nodes will be achieved by ECDHA for secure communication. Remaining paper is organized as follows: Next section deals about various routing protocols with their advantages and disadvantages. Section3 explain about various possible attacks in MANET. Section 4 describes short note about Related Work on MANET. Section 5 explicates about access control mechanism developed on ECC. In section 6 discussed our proposed mechanism. In section 7 will deals comparative results. In section 8 will give entitled conclusion to our approach.

2. ROUTING PROTOCOLS

Routing algorithms are used to establish the appropriate path between a pair of nodes on which a message may be delivered in a timely manner. The routing protocols allow the network to adjust dynamically to changing conditions. Routing basically involves packet transformation and optimal route finding. Forwarding packets uses the straight forward approach, but optimal route finding is very complex. Routing protocols uses many measurements to find best path for routing the packets from source to destination. Widely it uses hop count to find optimal path. Routing algorithms maintains routing table which contain information about route. The routing information varies from one to another. Generally routing table contains IP address and next hop. The information in routing table states that how particular destination can be reached optimally. For packet transfer, the router/node verifies the protocol address and forwards it to next neighbor node. Routing protocols are classified based on network topology and routing strategy. Pro-active or table-driven routing protocols maintain routing information even though it does not need communication. Each and every mode maintains the information about whole network. All nodes in the network should periodically update its routing table. The advantage is that the route to a particular destination is immediately available. But it is not suitable for larger network. They need maintain all node information. It may lead to consumption of more memory and bandwidth. Reactive or on-demand protocols don't maintain any routing information until it doesn't require any communication between nodes. Any node wants to communicate with other node, it searches route in an on demand and establish a connection to exchange the packets. It usually follows flooding the route request packet to the network. It stores only the routes which are required to establish a communication. The disadvantage is that it takes more time for route finding and more flooding leads to network clogging. A hybrid protocol combines the advantages of both proactive and reactive protocols. The routing is established with some proactively prospected routes and then serves the demands from additionally activated nodes through reactive flooding. The initial route discovery takes more delay but afterwards it will be very easy to maintain route even network breaks. Even, it consumes more network resources like processing power and bandwidth. In this paper, we are going to use DYMO [4] protocol. It provide better performance than available existing proactive routing protocols like DSDV and OLSR and reactive routing protocols AODV[1][2], DSR[5]. In subsequent section, DYMO protocols have been explained Next section describes about various attacks encountered in MANET.

3. ATTACKS IN MANET

The attacks in MANET can be categories into two major types: External attack and Internal attack, according the domain of the attacks. Some researchers consider as outsider and insider attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights. MANET has the following characteristics: autonomous terminal, distributed, multi-hop routing and dynamic network topology, spontaneous and mobile and thin mobile. Wired network supports firewall based security, but MANET does not support it, because there is no centralized node. MANET faces many attacks including eavesdropping, address spoofing, forged packets and denial of service (DOS). Attacks can come from any place and can target at any node inside the wireless network. MANET has the following characteristics: autonomous terminal, distributed, multi-hop routing and dynamic network topology, spontaneous and mobile and thin mobile. Wired network supports firewall based security, but MANET does not support it, because there is no centralized node. MANET faces many attacks including eavesdropping, address spoofing, forged packets and denial of service (DOS). Attacks can come from any place and can target at any node inside the wireless network.

Most network layer attacks against MANET networks fall into one of the following categories:

1. Spoofed, altered, or replayed routing information
2. Selective forwarding
3. Sinkhole attacks
4. Sybil attacks
5. Wormholes
6. HELLO flood attacks
7. Acknowledgement spoofing

3.1 Spoofed, altered, or replayed routing information.

The most direct attack against a routing protocol is to target the routing data exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc [19].

3.2 Selective Forwarding

In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ascertaining that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet she sees [20].

3.3 Sinkhole Attacks

In a sinkhole attack [16, 19], the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the opponent at the centre. Because nodes on, or near, the path that packets follow have many opportunities to fiddle with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example). Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. For instance, an adversary could spoof or replay an advertisement for an enormously high quality route to a base.

3.4 Sybil Attack

In a Sybil attack [16], a single node presents multiple individualities to other nodes in the network. The Sybil attack can significantly reduce the potency of fault-tolerant schemes such as distributed storage, disparity and multipath routing, and topology maintenance [23]. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities. Sybil attacks also pose a significantly threat to geographic routing protocols.

3.5 Hello Flood Attack

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false. An attacker with a high powered antenna can convince every node in the network that it is their neighbor. If the attacker also advertises a high quality route it can get every node to forward data to it. Nodes at a large distance from the attacker will be sending their messages into oblivion leaving the network in a state of confusion. This attack can also be thought of as a type of broadcast wormhole. Routing protocols dependent on localized information is extremely vulnerable to such attacks [19].

3.6 Acknowledgement Spoofing

Various MANET network routing algorithms rely on implicit or explicit link layer acknowledgements. Due to the constitutional broadcast medium, an adversary can spoof [24] link layer acknowledgments for "overheard" packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive. For example, a routing protocol may select the next hop in a path using link reliability. Artificially reinforcing a weak or dead line is a subtle way of manipulating such a scheme. Since packets sent along weak or dead links are lost, an adversary can effectively mount a selective forwarding attack using acknowledgement spoofing by encouraging the target node to transmit packets on those links.

4. RELATED WORK

To detect the resource consumption attacks, Jian-HuaSong, Fan Hong and Yu Zhang in [8] proposed a method to prevent the RREQs flooding by considering three parameters like rate limit, blacklist limit and delay timeout. Rafsanjani, Khavasi and Movaghar [6] proposed an IDS system for selecting the compromised node in the network using non interactive zero knowledge technique. They consider one node as an agent node having more resources like band width, power so that node will take care of compromised nodes. In Dai Hong, Li Haibo [15] proposed Network Intrusion Detection System (NIDS) which uses all data features that are irrelevant and redundant features. This can influence both the performance of the system and the types of attacks that NIDS detects. Selection algorithm based on Chi-Square and enhanced C4.5 algorithms to build lightweight network intrusion detection are also proposed. Verification test have been carried out by using the KDD Cup 1999[13][14] datasets. Guha, O.Kachirski and D.G.Schwartz [12] proposed a method which utilize cluster and cluster head employs the independent decision making. It also utilizes the mobile agent for communications among nodes. The intrusion detection engine is a case-based agent designed with the principle of artificial intelligence. by this method the efficient, bandwidth conscious, take into account of the distributed nature of MANET. But the disadvantage is Mobile agent's security is hard to implement, packet drop rate increase when network load increase. Sun B, K.wu and U.pooch [11] Implements an IDS which use collaboration mechanism in anomaly detection. In this model, a network is divided into logical zones. Each zone has a gateway node and individual nodes. Individual nodes has IDS agent working and detect intrusion activities individually. Once an individual node detects intrusion, it generates an alert message. Gate way node aggregates and correlates the alerts generated by the nodes in its zone. An algorithm is used in aggregate the alerts based on the similarities in the attributes of the alert. Only gateway nodes can utilize alert to in it alarm Nakayama, Kurosawa, Jamalipour, Nemoto and Nei Kato [9] proposed dynamic anomaly detection by using dynamic learning process. It involves the method to calculate the projection distance and compare it base line profile using PCA. Next section illustrates DYMO protocol.

5. ACCESS CONTROL MECHANISM

Transfer the information in confidential manner from nodes to the target node (base station) by using encryption methods. Even though there is possibility to divert the packets to other routes or specific node to drain out the limited energy. Nodes in MANET may be lost due to power exhaustion or malicious attacks. To extend the life time of MANET network, deployment of new nodes is necessary. To prevent malicious nodes from joining the MANET network, access control is required in the design of MANET network protocols. So in this situation we need to control the access rights of the MANET nodes. By using access control mechanism is able achieve authentication, integration and confidentiality. There by we can mitigate the attackers from spoofing, routing misbehavior and unauthorized access. We propose an access control protocol based on Elliptic Curve Cryptography (ECC) for MANET networks. Our access control mechanism includes not only identity like conventional methods but also takes bootstrap time into consideration. To provide the security we have to consider the two important factors, authentication and key establishing. ECC provides two popular

algorithms they are, Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic Curve Diffie-Hellman key algorithm. Each algorithm provides authentication and key establishing respectively. Usually access control mechanism needed in following scenarios, when handshaking of old node and new node, which will be discussed in new node deployment module and another scenario between two old nodes. We should consider the following parameters have given by certification authority (CA). Fq is a finite field over prime number, let us assume E is elliptic curve then prime field over curve represented as E (Fq), G point's generator of curve, n is the order of curve, T is bootstrapping time. Let Ni, Nj are two nodes, si is private key of node Ni then calculate public key as follows. Qi= si*G where G is generator function. Node Ni calculates signature according to elliptic curve digital signature algorithm. Generated signature is pair indicated as (li, mi). To convert binary sequence into integers Hash algorithm is needed. Node Ni is intended to send the message m to Nj. k is a random variable selected from integers.

5.1 Authentication Mechanism (ECDSA)

The following steps indicates signature generation algorithm.

1. Calculate e = HASH (m), where HASH is a Cryptographic hash function, such as SHA-1
2. Select a random integer k from [1,n − 1]
3. Calculate li = xi (mod n), where (xi, yi) = k * G. If S = 0, go to step 2
4. Calculate mi = k − 1(e + sili)(mod n). If s = 0, go to step 2
5. The signature is the pair (li, mi)

If node Ni sends message to Nj, to authenticate Ni, Nj should know the public key of Ni. The following procedure will explain about signature verification algorithm.

1. Verify that r and s are integers in [1,n − 1]. If not, the signature is invalid.
2. Calculate e = HASH (m), where HASH is the Same function used in the signature generation.
3. Calculate w = s −1 (mod n)
4. Calculate u1 = ew (mod n) and u2 = liw (mod n)
5. Calculate (xi, yi) = u1G + u2QA
6. The signature is valid if xi= li(mod n), invalid Otherwise

5.2 Key Sharing Mechanism (ECDH)

ECDH ensures secrete key between two parties by using their public data and private data. Third party does not know the private data by using any public data of node. Before establishing the shared key both parties should agree on domain parameters. Node can generate public key as Q=s*G. let (si, Qi) be the pair of the private key-public key of node Ni and (sj,Qj) be the pair of private key-public key of node Nj. the following steps explains algorithm for key establishing between two parties.

1. The end node Ni computes K = (xK, yK) = si * Qi
2. The end node Nj computes L = (xL, yL) = sj * Qj
3. Since si*Qi = si*sj*G = sj*si*G = sj*Qj. Therefore K = L and hence xK = xL
4. Hence the shared secret is xK

By integrating these two algorithms (ECDSA&ECDH) into routing transmit the data in secure manner via authentication and key sharing mechanism.

6. PROPOSED SCHEME: SECURE MECHANISM FOR DYMO ROUTING PROTOCOL BY USING ELLIPTIC CURVE CRYPTOGRAPHY

The routing protocols discussed above don't provide any security features against attackers. So the main goal is to ensure the secure mechanism for transmission in MANET. Hence, we proposed architecture for Secure Mechanism for DYMO Routing Protocol by using Elliptic Curve Cryptography (SMDRECC). To provide secure routing, it is needed to concentrate on both routing as well as security to the routing misbehavior, depending from flooding attacks etc. The proposed architecture for SMDRECC contains four modules. Three are horizontal modules and one is vertical module, vertical module already discussed above, which works on remaining three horizontal modules. Before using the network deployment of nodes should do in pre-deployment module, here the nodes should be loaded with digital certificate contains both node identity and geographic location assigned by certification authority and store the bootstrapping times, defined as the time taken to load itself to connect the network. Here we are using DYMO protocol for forwarding data. Finally in new node deployment there is a possibility for malicious nodes entry, so to avoid this we are using access control mechanism on ECC. It ensures security parameters like authentication, integrity and confidentiality.

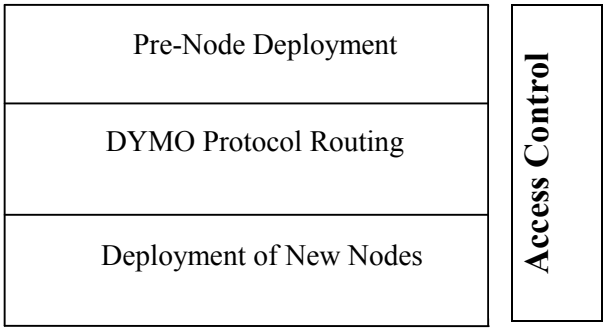

Figure2. Architecture for SMDRECC

6.1 Pre-node deployment

Before going to utilize the MANET network deploy the nodes manually. Deployment of nodes may be one time activity or continues process. If installation of nodes one time activity, then life time of network will expire in certain period of time. To extend the life time of MANET network, deployment of MANET should be continues process. This continues deployment will extends not only network life time but also extend the network. Placing of MANET categorized into two types, they are random manner and fixed manner. After deployment of wireless MANET, they have to load with parameters assigned by certification authority (CA) given above. Unlike traditional routing algorithms not only consider the identity of node (digital certificate which contains both node identity and geographic location of the node given by access

control mechanism) but also it considers bootstrapping time further security. Access control mechanism can be used in two scenarios, when one handshake happens between two new nodes (initial horizontal module- pre-node deployment) and another handshake happens between old node and new node (which will happens in new node deployment).

6.1.1 Handshaking between new nodes

This scenario will have to consider only after deployment of MANET (in pre-node deployment). We assume that all MANET nodes will maintain same bootstrapping times with tolerable values. Let t is the current time maintained by the legitimate nodes. If they will take loading time T after completion length of the bootstrapping time, present node time is determined as □T+□. Let we consider two nodes Ni, Nj digital certificate C asserted by certification authority (CA). Each node checks neighbor node identity and the nodes shares shared keys by using Diffie-Hellman key algorithm. Here we consider one more parameter bootstrapping time for more security. Authentication process as follows, one node checks identity of digital certificate (consist of node location and identity) and bootstrapping time.

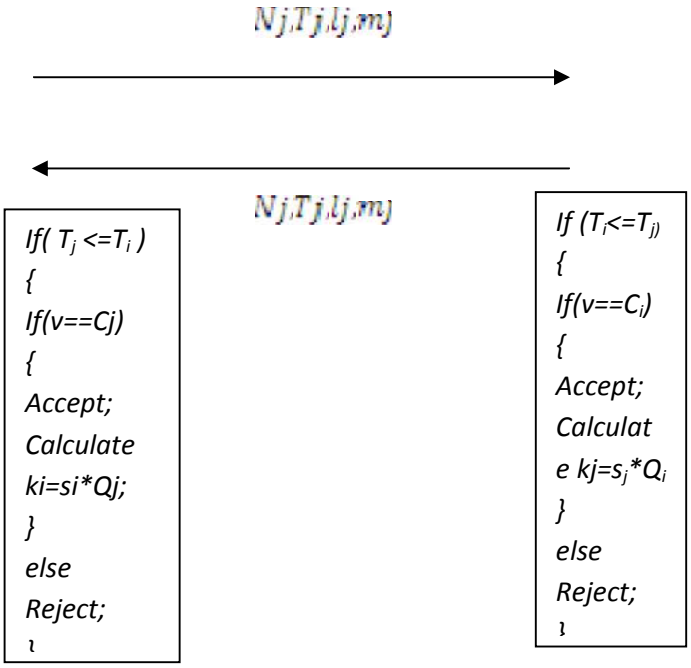

Figure3. handshake between two new nodes, both nodes should authenticate eachother.

6.2 DYMO Routing

DYMO (Dynamic On Demand) routing protocol is a recently proposed protocol defined in Internet Engineering Task Force (IETF) and DYMO is successor to the AODV routing protocol and shares many of its features. DYMO can work on both proactive and reactive protocols. Figure.4. shows the functions of AODV protocol and Figure 5 shows DYMO routing protocol. The basic operations of the DYMO protocol are route discovery and route maintenance. During these two operations we should use the access control mechanism for node identity and verification of access rights. In route discovery process, the source node will broadcast RREQ (Route Request) packet to its adjacent nodes. Before forwarding the information to the next node towards destination both nodes will verifies by using handshaking mechanism of two nodes as discussed above in section 4. Here the sending node verifies the identity of node signature of receiver node, bootstrapping time of the receiver and receiver node also verifies the digital signature of its own with other sending node. If the forwarding node having legitimate node identity then sender node will grant the permission to forward the data, thereby we can avoid the selecting forwarding attack. In the same way receiver node will verifies the sending node identity, so the receiver node is able to forward or receive the legitimate information to or from other adjacent nodes thereby this procedure will mitigate the flooding attack, sinkhole attack and wormhole attack.

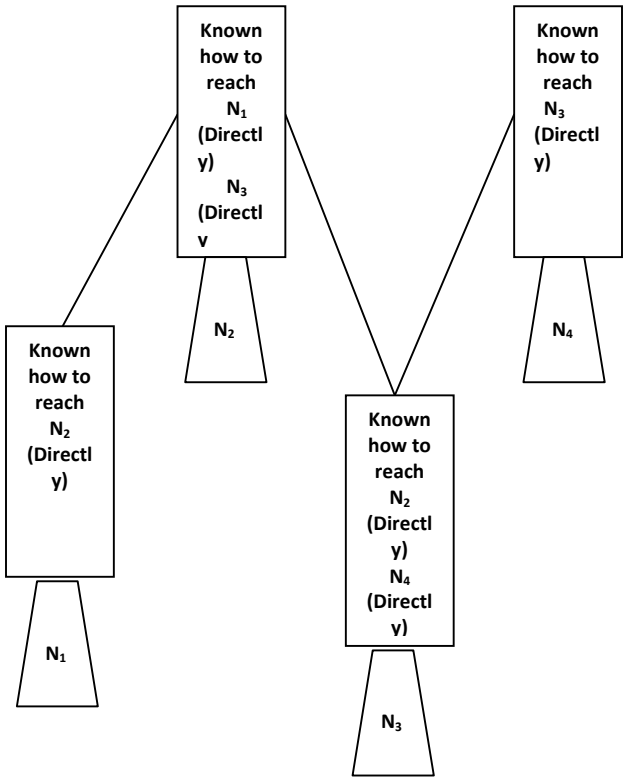

Figure.4. AODV Protocol

This procedure will continue until the information reach to the destination. The intermediate nodes will check the IP address of packet and forwards to next node. At the same time, it will store details of, from where it arrives and sequence number of the packet to avoid the looping. When the destination node receives the RREQ packet, it responds with RREP (Route Response) packet. The RREP packet will follow the same path from where it received RREQ during this period same authentication mechanism applied for secure communication. When source node receives the RREP, the new route has been established between source and destination. In route maintenance process, whenever any changes occur in the network, the node will send RRER (Route Error) towards the source node, when the source node receive RRER packet immediately source node reinitiate the route discovery process.

As mentioned earlier, MANET is collection of mobile hosts which can communicate without centralized administrative controller. So there is a chance of malicious node present in the

network, which can harm the network. With the aid of general cryptography techniques, the user can block the malicious nodes, even though it is very difficult to identify the malicious nodes within the network.

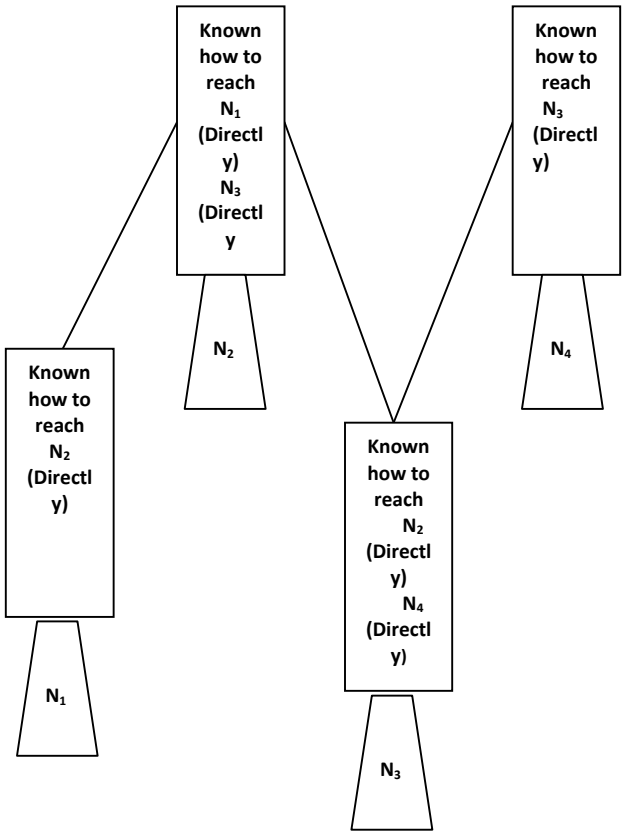

Figure.5. DYMO Protocol

Generally the attackers are classified into passive and active attackers. The passive attackers like eavesdroppers secretly listen to the private conversation of the user without their consent. Whereas active attackers will do repletion, changing or deletion of data which leads to congestion, distribution of incorrect routing information by changing the source IP address, destination IP address, RREQ IDs, hop count, destination sequence number and also flooding the network with routing packets. Comparison of DYMO protocol [10] with other routing protocols, DYMO provides better performance in terms of throughput, packet loss and latency. Even any link breaks in network, the route can be established very easily. During route discovery, each node in the route maintains information about routing nodes. In AODV, each node has the information about adjacent nodes only.

6.2.1 Working Functionality of Network Routing

In proposed DYMO routing protocol, source node send request to the target node that desire to send. The sender node selects the adjacent node which is very nearer with minimum distance. This minimum distance calculated by using Link State Routing algorithm. If the destination node is adjacent then source node checks the bootstrapping time and digital certificate of the target node. This If the imposed conditions met by the target node then it establish the shared key between two parties later it will send the Route request message. If the destination node is not adjacent the source node it checks the same conditions and forward the route request message to the intermediate nodes. This procedure repeats until the destination node find. While forwarding route request message from one node to the next node, it add the own address to the route request message. Upon receiving route request message from source node the target node responds with acknowledgement or route reply message. Target node keep track of source path, and it checks the node identity and source node id. If these two conditions met, the route reply message would get reached the source node. For more clarity on this refer figure.6.

6.3 Deployment of New Nodes

It is last module of SRECWSN architecture. Deployment of nodes may be one time activity or continues process. To extend the life time of network deployment of MANET nodes should be continues, so new deployment module is needed to install new nodes with existing nodes. It is useful for not only for extend the network length but also to replace nodes those will get repair. New node deployment will give the way for attackers to deploy the malicious nodes. The attacker act as new node act as legitimate one. To mitigate the actions of attackers we have to use the authentication mechanism. Here the communication will be taking in between old node and new node. The old should authenticate new node by verifying its identity and if the signature is valid it will checks the bootstrapping time of the new node. If it satisfies the tolerate value of bootstrapping time then old node allows to connect with network. Otherwise if it is not satisfy both conditions, old node simply discards the new node request. Consider below scenario (figure.6) for more information. Consider the bellow scenario, the new node identity Ni and the old node identity Nj. The new node will have to generate the public key and private key that should be lies in range of prime field. Here the old node (neighbor node in network which is nearer) should follow the ECDSA to authenticate the identity of old node. The new node will generate the signature by using public key and private key. The node generates public key, by multiplying random generator number with private key.

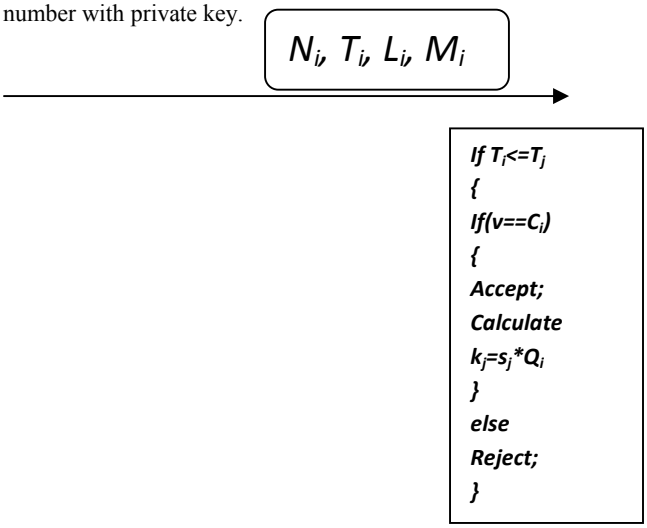

Figure7. shows handshake between old node and new node

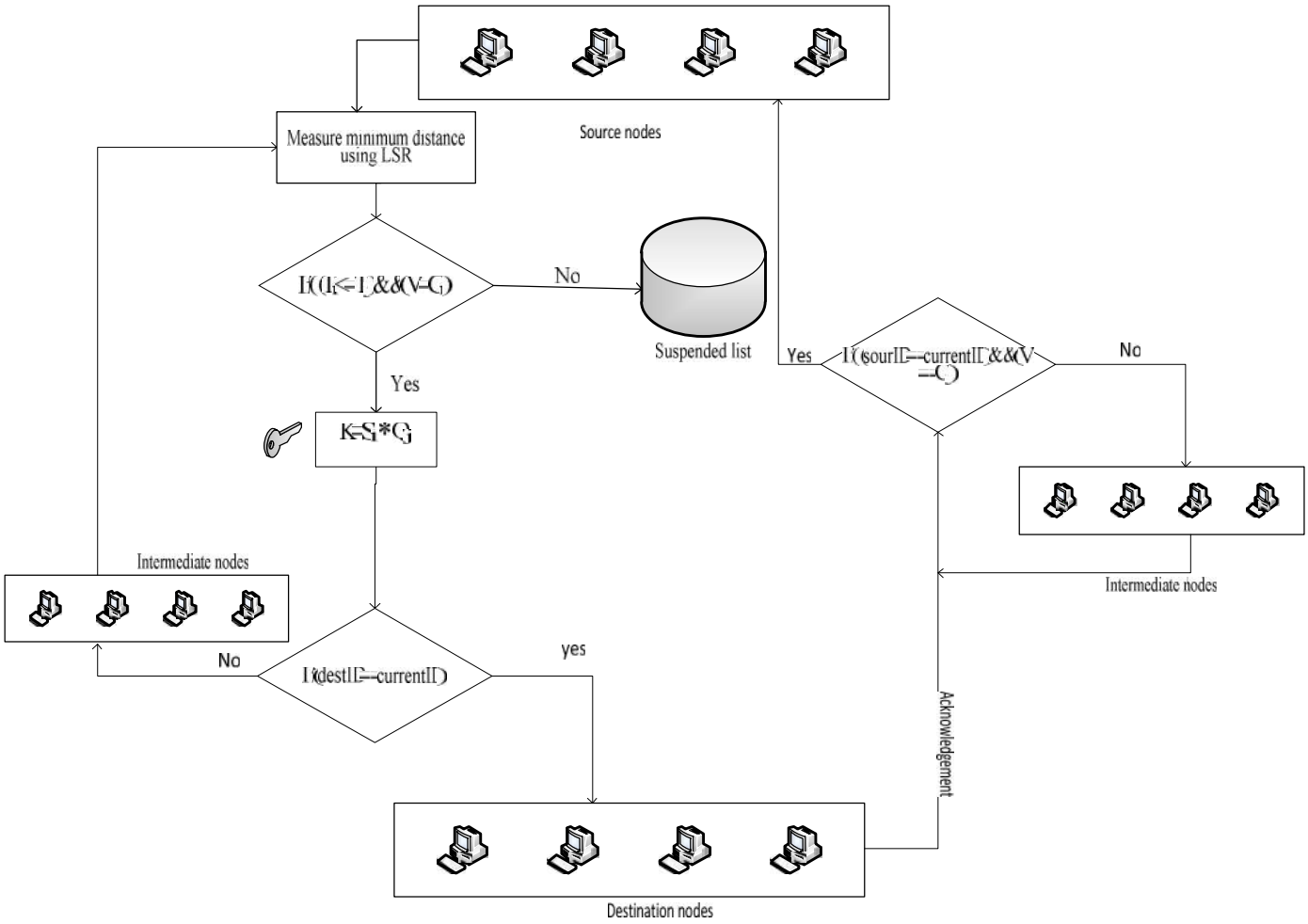

Figure.6. Network Routing in SMDRECC

Table-1

PARAMETER	DYMO WITH ECC	SEAD	SRP
Number of CBR data packets produced	1145	681	652
Number of UDP data packets generate	18028	1497	5
Number of CBR data packet send	586	584	584
Number of UDP data packet send	9090	760	05
Number of dropped Packets	328	513	510
Number of forwarded packets	0	109	78

Packet delivery ratio (CBR and UDP) in %	0.98	0.62	0.12
Data packet lost	174	505	512
Average Delay	1.583	2.474	1.696
Control packet forwarded	0	09	01
Normalized routing load	7.95	6.69	40.789

7. SIMULATION AND EVALUATION OF RESULTS

This section describes the simulation tool and parameters chosen to simulate the routing protocols. In this paper the Fedora 12 Operating System was used because it is a user-friendly platform and easy to manage and to setup a simulator. For simulation software, Network Simulation NS2.34 was used as the simulator to evaluate the performance of SEAD (Secure Efficient Ad-Hoc Distance Vector Routing Protocol), SRP and DYMO with ECC routing protocols. In this project, the simulation environment consist of two different number of nodes which are 3, 6. We have simulated the entire above mentioned algorithm under different condition. In first simulation environment we have created 6 nodes and for node movement we have used seed. Constant Bit Rate (CBR) traffic generators is used as sources to run the simulation when node 0 is source and 3 is destination and FTP is used when node 0 is source and node 1 is destination. Each CBR packet contained 512 Bytes and packets were transmitted at 20Kb and FTP of 960 Bytes at 0.01Kb. Parameters used in simulations are shown in Table-1. We compare access control mechanism on elliptic curve cryptography with popular RSA algorithm. ECC is giving more security compare to RSA, which is taking fewer bits key and providing more security. ECC is seen to be the standard for the next generation cryptographic technology. The reason is that ECC can achieve the same level of security with smaller key sizes. It has been shown that 160-bit ECC provides comparable security to 1024-bit RSA and 224-bit ECC provides comparable security to 2048-bit RSA. Under the same security level, smaller key sizes of ECC offer merits of faster computational efficiency, as well as memory, energy and bandwidth savings.

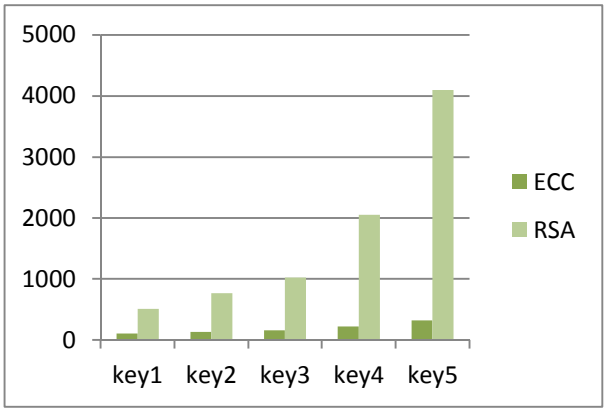

Figure.8. security comparison of key size's of ECC with RSA

Here x- axis represents the key number and y- axis represents key size.

7.1 Performance evaluation of DYMO with ECC

We consider two protocols SEAD and SRP for comparison of performance evaluation with secure DYMO protocol. In Elliptic Curve Cryptography we chosen ECDSA (Elliptic Curve Digital Signature Algorithm) for authentication and Elliptic Curve Diffie-Hellman key algorithm for establishing shared key between two parties thereby we can achieve both authentication and confidentiality through these algorithms. We selected experimental setup with various numbers of nodes in different secure protocols. Here we injected malicious nodes to compromise the identity of nodes or divert the routing information. Plotted the graph with output of these experimental results, the number of compromised nodes has taken on x-axis and simulation time has taken on y-axis. From the results our protocol has supported for large scale networks with good performance and data transmitted in secure manner. Remaining protocols are not capable to support large scale networks, but which are more effective in small organizations.

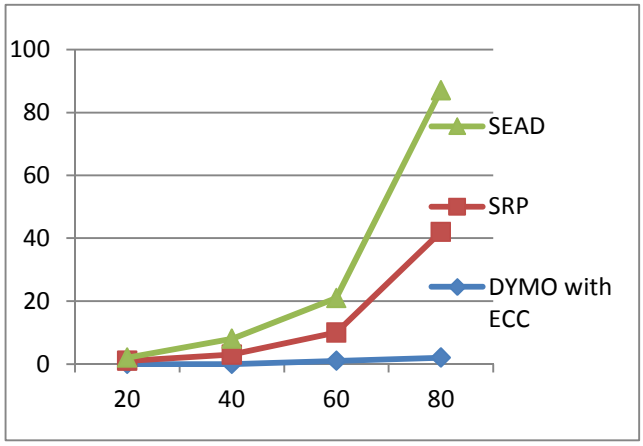

Figure.9. Comparison of compromised nodes in DYMO routing protocol

X-axis represents simulation time and Y-axis represents number nodes in network.

8. CONCLUSION

Secure routing is vital to the acceptance and use for many MANET network applications. In this research work, we implemented DYMO routing protocol with integration of Elliptic Curve Cryptography to ensure security for the routing information. It has given extensive security over RSA

encryption algorithm and also it is suitable for low power devices like MANET and sensor nodes. Unlike conventional method that try to prevent the malicious node after joining the network, but our proposed access control mechanism prevent attackers before joining the network. Our proposed scheme justified by considering the different parameters like number of CBR packets sent, UDP packets, average delay, data lost in packets and normalizing routing load etc in simulation with 100 nodes. By using our proposed scheme we have increased the network life time, packets sent and number of packets dropped through mitigation of intruders and malicious nodes from network. Here it will allow adding new nodes to the existing network, so this kind of process increase the life time of the network and provides efficient secure transmission of data over SEAD and SRP protocols.

9. REFERENCES

[1] Clausen T., Jacquet P., Viennot L., "Comparative study of CBR and TCP performance of MANET routing protocols", Project HiPERCOM – INRIA, France, 2003.

[2] Grew P., Giudici F., Pagani E."Specification of a functional architecture for e-learning supported by wireless technologies‖, Pervasive Computing and Communications Workshops, 2006. PerCom Workshops 2006. Fourth Annual IEEE International Conference on Volume, Issue, 13-17 March 2006 Page(s):5 pp. – 220

[3] Hogie L., Bouvry P., ―An overview of MANET Simulation‖, Electronic notes in theoretical computer science, © 2006 Elsevier, doi:10.1016/j.entcs.2005.12.025.

[4] E Belding-Royer, I Chakeres, D. Johnson and C Perkins, "DyMO – dynamic MANET on-demand routing protocol," Proceedings of the Sixty-First Internet Engineering Task Force, Washington, DC, USA, November 2004. IETF.

[5] D. B. Johnson, D. A. Maltz, and Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Jul. 2004, NTERNET-DRAFT draft-ietf-manet-dsr-10.txt. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[6] Marjan Kuchaki Rafsanjani, Ali Asghar Khavasi and Ali Movaghar,"An Efficient Method for Identifying IDS Agent Nodes by Discovering Compromised Nodes in MANET" in proc ICCEE , Vol.01., pp.625-629, December 2009.

[7] Adnan Nadeem and Michael Howarth ,"Adaptive intrusion detection & preventing of denial of service attacks in MANET", ACM, pp.926-930, 2009.

[8] Jian-HuaSong, Fan Hong and Yu Zhang," Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 497-502 ,2006.

[9] Hidehisa Nakayama,Satosi Kurosawa, Abbas Jamalipour,Yoshiaki Nemoto and Nei Kato, " A Dynamic Anomaly Detection Scheme For AODV- Based Mobile AdHoc Networks", IEEE Transactions On Vehicular Technology,Vol.58, No. 5, pp.2471-2481, June 2009.

[10] Dong-Won Kum, Jin-Su Park, You-Ze Cho and Byoung-Yoon Cheon," Performance Evaluation Of AODV and DYMO Routing Protocols in MANET", in proc IEEE CCNC, Las Vegas, Nevada, USA, pp.1046-1047, Jan.2010.

[11] C.K.Toh,"Ad-Hoc mobile wireless network protocol and system", Pearson Education, 2009.

[12] Dai Hong, Li Haibo.A Lightweight Network Intrusion Detection Model Based on Feature Selection. DOI 10.1109/PRDC.2009.34,p.p 165-168.

[13] Wanli Ma, Dat Tran, Dharmendra Sharma,"A Study on the Feature Selection of NetworkTraffic for Intrusion Detection Purpose"p.p 245-247,2008, Taipei, Taiwan.

[14] ACM. KDD CUP 1999 data. [Cited 12 January 2007]; Available from: http://kdd.ics.uci.edu//databases/kddcup99/kddcup99.html.

[15] H. Liu, Setiono and R., "Chi2: feature selection and discretization of numeric attributes", in Proc of the Seventh International Conference on Tools with Artificial Intelligence, pp. 388 - 391, 1995.

[16] Hemanta Kumar Kalita, Avijit Kar, "Wireless Sensor Network Security Analysis," International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009,1-9.

[17] Yan Yu, Ramesh Govindan, Deborah Estrin, "Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks," Aug 2001.

[18] Brad Karp, H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," MobiCom 2000.

[19] Pooja Sharma, Pawan Bhadana, "An Effective Approach for Providing Anonymity in Wireless sensor Network: Detecting Attacks and Security Measures," (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1830-1835.

[20] Shivangi Raman, Amar Prakash, Kishore Babu Pulla, Prateek Srivastava, Ashish Srivastava, Shveta Singh, "Wireless sensor networks: A Survey of Intrusions and their Explored Remedies," International Journal of Engineering Science and Technology Vol. 2(5), 2010, 962-969.

[21] Zaw Tun and Aung Htein Maw, "Wormhole Attack Detection in Wireless Sensor Networks," orld Academy of Science, Engineering and Technology 46 2008, 545-550.

[22] Yun Zhou, Yanchao Zhang, Yuguang Fang, "Access control in wireless sensor networks," Ad - hoc Networks 5 (2007) 3–13.

[23] Jiang Du, Su Peng, "Choice of Secure Routing Protocol for Applications in Wireless Sensor Networks," 2009 International Conference on Multimedia Information Networking and Security.

[24] Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Ad Hoc Networks 1 (2003) 293–315.

[25] Fan Ye, Alvin Chen, Songwu Lu, Lixia Zhang, "A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks," in Tenth International Conference on Computer Communications and Networks, 2001, pp. 304–309.

[26] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: Ascalable and robust communication paradigm for sensor networks," in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM '00), August 2000,58-67.

[27] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review,oct 2001, Volume 1, Number 2,1-13.

[28] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Micro sensor Networks," Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.

[29] D. Braginsky and D. Estrin, "Rumour routing algorithm for sensor networks," in First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.

[30] Zhen Yu, Member, IEEE, and Yong Guan, Member, IEEE, "A Dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks," IEEE/ACM Transactions on Networking, Vol. 18, No. 1, February 2010,150-163.